日本国特許庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日
Date of Application: 1999年11月30日

出願番号
Application Number: 平成11年特許願第341288号

パリ条約による外国への出願に用いる優先権の主張の基礎となる出願の国コードと出願番号
The country code and number of your priority application, to be used for filing abroad under the Paris Convention, is JP1999-341288

出願人
Applicant(s): 株式会社リコー

2005年 5月 2日

特許庁長官
Commissioner,
Japan Patent Office

小川洋

出証番号 出証特2005-3039288

【書類名】　特許願

【整理番号】　9907601

【提出日】　平成11年11月30日

【あて先】　特許庁長官殿

【国際特許分類】　G09C　1/00

G06F 12/14

【発明の名称】　電子情報公開証明方法及びシステム、並びに電子情報公開証明プログラムを格納した記憶媒体

【請求項の数】　28

【発明者】

【住所又は居所】　東京都大田区中馬込１丁目３番６号

株式会社　リコー内

【氏名】　金井　洋一

【発明者】

【住所又は居所】　東京都大田区中馬込１丁目３番６号

株式会社　リコー内

【氏名】　谷内田　益義

【発明者】

【住所又は居所】　東京都大田区中馬込１丁目３番６号

株式会社　リコー内

【氏名】　水野　富夫

【発明者】

【住所又は居所】　東京都大田区中馬込１丁目３番６号

株式会社　リコー内

【氏名】　古川　達也

【発明者】

【住所又は居所】　東京都大田区中馬込１丁目３番６号

株式会社　リコー内

【氏名】　石川　洋一

【特許出願人】

【識別番号】　000006747

【氏名又は名称】　株式会社　リコー

【代表者】　桜井　正光

【手数料の表示】

【予納台帳番号】　003724

【納付金額】　21,000円

【提出物件の目録】

【物件名】　明細書　1

【物件名】　図面　1

【物件名】　要約書　1

【プルーフの要否】　要

【書類名】　明細書

【発明の名称】　電子情報公開証明方法及びシステム、並びに電子情報公開証明プログラムを格納した記憶媒体

【特許請求の範囲】

【請求項１】　ネットワークに接続された特定のコンピュータにおいて特定の電子情報が公開されていたことを証明する方法であって、

記録依頼に応じて、前記特定のコンピュータに格納された前記特定の電子情報にアクセスし、前記特定の電子情報をコピーするステップと、

コピーされた前記特定の電子情報及び前記ネットワーク上における前記特定の電子情報の所在に関する情報を含む属性情報を日時と共にユニークに特定し且つ認証する電子証明書を取得し、当該電子証明書及び前記属性情報を記憶装置に格納するステップと、

前記記憶装置に格納された前記電子証明書及び前記属性情報を当該証明依頼元に提供するステップと、

を含むことを特徴とする電子情報公開証明方法。

【請求項２】　ネットワークに接続された特定のコンピュータにおいて特定の電子情報が公開されていたことを証明する方法であって、

記録依頼に応じて、前記特定のコンピュータに格納された前記特定の電子情報に所定のタイミングでアクセスし、アクセスするごとに前記特定の電子情報をコピーする第１ステップと、

コピーされた前記特定の電子情報及び前記ネットワーク上における前記特定の電子情報の所在に関する情報とアクセス条件とを含む属性情報を日時と共にユニークに特定し且つ認証する電子証明書を取得し、当該電子証明書及び前記属性情報を記憶装置に格納する第２ステップと、

を含むことを特徴とする電子情報公開証明方法。

【請求項３】　前記電子証明書に対応して、最初にコピーされた前記特定の電子情報を記憶装置に格納する第３ステップをさらに含むことを特徴とする請求項２記載の電子情報公開証明方法。

【請求項４】　前記記憶装置に格納された前記電子証明書及び前記属性情報を証明依頼元に提供する第４ステップをさらに含むことを特徴とする請求項２記載の電子情報公開証明方法。

【請求項５】　前記第４ステップが、前記電子証明書に対応する前記特定の電子情報を前記証明依頼元に提供するステップを含むことを特徴とする請求項４記載の電子情報公開証明方法。

【請求項６】　前記第１ステップが、前記特定のコンピュータに格納された前記特定の電子情報に所定のタイミングで且つアクセス元のアドレスを変更しつつアクセスするステップを含むことを特徴とする請求項２記載の電子情報公開証明方法。

【請求項７】　前記第１ステップが、前記特定のコンピュータに格納された前記特定の電子情報に所定のタイミングで且つ所定の頻度でアクセスするステップを含むことを特徴とする請求項２記載の電子情報公開証明方法。

【請求項８】　前記特定の電子情報をアクセス可能とするための参照情報を前記特定のコンピュータ以外の前記ネットワークに接続されたコンピュータに保持させるステップをさらに含むことを特徴とする請求項２記載の電子情報公開証明方法。

【請求項９】　コピーされた前記特定の電子情報の変更の有無を検出するステップと、

変更があることを検出した場合には、当該変更があったということを記憶装置に格納するステップと、

をさらに含むことを特徴とする請求項２記載の電子情報公開証明方法。

【請求項１０】　前記記憶装置に格納された前記特定の電子情報を検索可能なように前記ネットワーク上の前記特定のコンピュータ以外のコンピュータで公開するステップをさらに含むことを特徴とする請求項３記載の電子情報公開証明方法。

【請求項１１】　前記記憶装置に格納された前記特定の電子情報の要約を検索可能なように前記ネットワーク上の前記特定のコンピュータ以外のコンピュータで公開するステップをさらに含むことを特徴とする請求項３記載の電子情報公

開証明方法。

【請求項１２】　前記特定の電子情報が前記ネットワーク上で提供されている電子情報検索手段により検索可能である場合には、当該検索可能であるということを記憶装置に格納するステップをさらに含むことを特徴とする請求項２記載の電子情報公開証明方法。

【請求項１３】　前記ネットワークがインターネットであり、

前記電子情報はマークアップ・ランゲージにより記述された文書であり、

前記ネットワーク上における前記電子情報の所在に関する情報はユニフォーム・リソース・ロケータであり、

前記アクセス条件は、少なくともアクセス元のＩＰアドレスを含むことを特徴とする請求項２記載の電子情報公開証明方法。

【請求項１４】　ネットワークに接続された特定のコンピュータにおいて特定の電子情報が公開されていたことを証明するシステムであって、

記録依頼に応じて、前記特定のコンピュータに格納された前記特定の電子情報にアクセスし、前記特定の電子情報をコピーする手段と、

コピーされた前記特定の電子情報及び前記ネットワーク上における前記特定の電子情報の所在に関する情報を含む属性情報を日時と共にユニークに特定し且つ認証する電子証明書を取得し、当該電子証明書及び前記属性電子情報を記憶装置に格納する手段と、

前記記憶装置に格納された前記電子証明書及び前記属性電子情報を提供する手段と、

を有することを特徴とする電子情報公開証明システム。

【請求項１５】　ネットワークに接続された特定のコンピュータにおいて特定の電子情報が公開されていたことを証明するシステムであって、

記録依頼に応じて、前記特定のコンピュータに格納された前記特定の電子情報へ所定のタイミングでアクセスし、アクセスするごとに前記特定の電子情報をコピーするアクセス手段と、

コピーされた前記特定の電子情報及び前記ネットワーク上における前記特定の電子情報の所在に関する情報とアクセス条件とを含む属性情報を日時と共にユニ

ークに特定し且つ認証する電子証明書を取得し、当該電子証明書及び属性情報を記憶装置に格納する手段と、

前記記憶装置に格納された前記電子証明書及び前記属性情報を当該証明依頼元に提供する発行手段と、

を有することを特徴とする電子情報公開証明システム。

【請求項１６】　前記電子証明書を発行する手段をさらに有することを特徴とする請求項１５記載の電子情報公開証明システム。

【請求項１７】　前記記憶装置が、前記電子証明書に対応して、最初に取得された前記特定の電子情報のコピーを格納することを特徴とする請求項１５記載の電子情報公開証明システム。

【請求項１８】　前記提供手段が、前記電子証明書に対応する、前記記憶装置に格納された前記特定の電子情報を前記証明依頼元に提供することを特徴とする請求項１７記載の電子情報公開証明システム。

【請求項１９】　前記アクセス手段が、前記特定のコンピュータに格納された前記特定の電子情報に所定のタイミングで且つアクセス元のアドレスを変更しつつアクセスするをことを特徴とする請求項１５記載の電子情報公開証明システム。

【請求項２０】　前記アクセス手段が、前記特定のコンピュータに格納された前記特定の電子情報に所定のタイミングで且つ所定の頻度でアクセスすることを特徴とする請求項１５記載の電子情報公開証明システム。

【請求項２１】　前記特定の電子情報をアクセス可能とするための参照情報を格納し、前記ネットワークに接続した、前記特定のコンピュータ以外のコンピュータ　をさらに含むことを特徴とする請求項１５記載の電子情報公開証明システム。

【請求項２２】　コピーされた前記特定の電子情報の変更の有無を検出し、変更があることを検出した場合には、当該変更があったということを前記記憶装置に格納する手段をさらに有することを特徴とする請求項１５記載の電子情報公開証明システム。

【請求項２３】　前記特定の電子情報を格納し且つ検索可能とする、前記ネ

ットワークに接続した、前記特定のコンピュータ以外のコンピュータをさらに有することを特徴とする請求項１５記載の電子情報公開証明システム。

【請求項２４】　前記特定の電子情報の要約を格納し且つ検索可能とする、前記ネットワークに接続した、前記特定のコンピュータ以外のコンピュータをさらに有することを特徴とする請求項１５記載の電子情報公開証明システム。

【請求項２５】　前記記憶装置が、前記特定の電子情報が前記ネットワーク上で提供されている電子情報検索手段により検索可能である場合には、当該検索可能であるということを格納することを特徴とする請求項１５記載の電子情報公開証明システム。

【請求項２６】　前記ネットワークがインターネットであり、

前記電子情報はマークアップ・ランゲージにより記述された文書であり、

前記ネットワーク上における前記電子情報の所在に関する情報はユニフォーム・リソース・ロケータであり、

前記アクセス条件は、少なくともアクセス元のＩＰアドレスを含むことを特徴とする請求項１５記載の電子情報公開証明システム。

【請求項２７】　ネットワークに接続された特定のコンピュータにおいて特定の電子情報が公開されていたことを証明するためのプログラムを格納した記憶媒体であって、

前記プログラムは、

前記特定のコンピュータ以外のコンピュータに、記録依頼に応じて、前記特定のコンピュータに格納された前記特定の電子情報にアクセスし、前記特定の電子情報をコピーするステップと、

コピーされた前記特定の電子情報及び前記ネットワーク上における前記特定の電子情報の所在に関する情報を含む属性情報を日時と共にユニークに特定し且つ認証する電子証明書を取得し、当該電子証明書及び前記属性情報を記憶装置に格納するステップと、

前記記憶装置に格納された前記電子証明書及び前記属性情報を当該証明依頼元に提供するステップと、

を含むことを特徴とする記憶媒体。

【請求項２８】　ネットワークに接続された特定のコンピュータにおいて特定の電子情報が公開されていたことを証明するためのプログラムを格納した記憶媒体であって、

前記プログラムは、

前記特定のコンピュータ以外のコンピュータに、記録依頼に応じて、前記特定のコンピュータに格納された前記特定の電子情報に所定のタイミングでアクセスし、アクセスするごとに前記特定の電子情報をコピーする第１ステップと、

コピーされた前記特定の電子情報及び前記ネットワーク上における前記特定の電子情報の所在に関する情報とアクセス条件とを含む属性情報を日時と共にユニークに特定し且つ認証する電子証明書を取得し、当該電子証明書及び前記属性情報を記憶装置に格納する第２ステップと、

を含むことを特徴とする記憶媒体。

【発明の詳細な説明】

【０００１】

【発明が属する技術分野】

本発明は、ネットワーク上の電子情報が公開されていたことを証明するための方法、システム及びプログラム並びに該プログラムを格納した記録媒体に関する。

【０００２】

【従来の技術】

従来から、ある電子情報が特定の日時に存在していたことを認証する方法及びシステムは存在していた。このような方法及びシステムは、例えば米国特許第５１３６６４７号、米国再審査特許第ＲＥ３４９５４号、米国特許第５１３６６４６号、米国特許第５３７３５６１号、米国特許第５７８１６２９号などに記載されている。

しかし上述の米国特許に示された技術は、例えばインターネット等で、特定の電子情報が公開されていたことを証明するものではない。

【０００３】

【発明が解決しようとする課題】

近年、インターネット等でも技術情報が開示されるようになり、このような技術情報は、雑誌や図書等の形で刊行された技術情報と同等の内容の情報を含んでおり、その伝達の迅速性等は従来の刊行物とは比較にならないほどである。よって、研究者が自己の研究成果を早期に公表すること等を目的としてインターネット等を使用することも多くなっている。また、従来の刊行物に比して情報の発信が簡便であり、コストも低いため、より多くの情報がインターネット等で公開される可能性が高い。しかし、従来技術では電子情報が存在していたことを証明することはできるが、インターネット等で公開されていたということを証明することはできなかった。すなわち、電子情報が秘密であったかどうかを判別することができなかった。

斯かる場合、即ちインターネット等で公開されていたということを証明することができない場合には、公開されていた技術内容と同様の内容の特許を他人が取得してしまうという恐れがある。上述の通り、インターネット等で公開された技術情報は、実質的に刊行物と同じ効果を奏するものであり、日本においては「電子通信回線を通じて公衆に利用可能になった発明」に対しては特許を与えないような法律が制定されている。しかし、インターネット等で公開された技術情報は、いつ公開されていたのか、改ざんされていないのか、という事実を証明することが困難であるため、証拠としての信頼性が従来の刊行物に比して弱い、という面は否めない。

そこで、本発明は、インターネット等のネットワーク上で、ある特定の電子情報が所定の条件の下公開されていたことを証明するための方法、システム及びコンピュータ・プログラム並びに該コンピュータ・プログラムを格納した記録媒体を提供することを目的とする。

【０００４】

【課題を解決するための手段】

本発明の第１の態様に係る、ネットワークに接続された特定のコンピュータにおいて特定の電子情報が公開されていたことを証明する方法は、記録依頼に応じて、特定のコンピュータに格納された当該特定の電子情報にアクセスし、特定の電子情報をコピーするステップと、コピーされた特定の電子情報及びネットワー

ク上における特定の電子情報の所在に関する情報を含む属性情報を日時と共にユニークに特定し且つ認証する電子証明書を取得し、当該電子証明書及び属性情報を記憶装置に格納するステップと、記憶装置に格納された電子証明書及び属性情報を当該証明依頼元に提供するステップとを含む。これにより、証明書の日時で且つ属性情報に含まれる所在に関する情報（例えばＵＲＬ（Uniform Resource Locator））で指定された場所の電子情報にアクセスできたことが証明できるようになる。

本発明の第２の態様に係る電子情報公開証明方法は、記録依頼に応じて、特定のコンピュータに格納された前記特定の電子情報に所定のタイミングでアクセスし、アクセスするごとに特定の電子情報をコピーする第１ステップと、コピーされた特定の電子情報及びネットワーク上における特定の電子情報の所在に関する情報とアクセス条件とを含む属性情報を日時と共にユニークに特定し且つ認証する電子証明書を取得し、当該電子証明書及び属性情報を記憶装置に格納する第２ステップとを含む。このようにすれば、電子情報が一定期間ネットワーク上で公開されていることを合わせて証明できるようになる。

また、本発明の第２の態様において、電子証明書に対応して、最初にコピーされた当該特定の電子情報を記憶装置に格納する第３ステップをさらに含むような構成も可能である。記録依頼元で電子情報を保管しておくことも可能であるが、本実施態様においては、証明書等と共に一元管理するようにしている。

さらに、本発明の第２の態様において、記憶装置に格納された電子証明書及び属性情報を当該証明依頼元に提供する第４ステップをさらに含むような構成も可能である。

また、上で述べた第４ステップを、電子証明書に対応する当該特定の電子情報を証明依頼元に提供するステップを含むように構成することも可能である。

また、上で述べた第１ステップを、特定のコンピュータに格納された特定の電子情報に所定のタイミングで且つアクセス元のアドレスを変更しつつアクセスするステップを含むように、又は特定のコンピュータに格納された特定の電子情報に所定のタイミングで且つ所定の頻度でアクセスするステップを含むように構成することも可能である。アクセス元アドレスの変更を行うことにより、不特定の

コンピュータからアクセスできることの証明ができるようになる。また、所定の頻度でアクセスすることにより、電子情報の変更などについて捕捉し易くなる。

【０００５】

本発明の第２の態様において、特定の電子情報をアクセス可能とするための参照情報を特定のコンピュータ以外のネットワークに接続したコンピュータに保持させるステップをさらに含むように構成することも可能である。この参照情報によって一般公衆が電子情報の所在を容易に得ることができるようになり、電子情報の公衆による利用可能性を向上することができる。この参照情報が存在することも何らかの形で証明できるようにすることが好ましい。

また本発明の第２の態様において、コピーされた当該特定の電子情報の変更の有無を検出するステップと、変更があることを検出した場合には、当該変更があったということを記憶装置に格納するステップとをさらに含むような構成も可能である。これにより、電子情報のバージョン遷移の記録が可能になる。

さらに本発明の第２の態様において、記憶装置に格納された電子情報を検索可能なようにネットワーク上の当該特定のコンピュータ以外のコンピュータで公開するステップをさらに含むような構成も可能である。電子情報の公衆による利用性をより高めることができ、さらに第三者も証明書付の電子情報を使用することができるようになる。これに関連して、記憶装置に格納された電子情報の要約を検索可能なようにネットワーク上の当該特定のコンピュータ以外のコンピュータで公開するステップをさらに含むような構成も可能である。

本発明の第２の態様において、前記特定の電子情報をネットワーク上で提供されている電子情報検索手段により検索が可能である場合には、当該検索が可能であるということを記憶装置に格納するステップをさらに含むような構成も可能である。その特定の電子情報を電子情報検索手段により検索が可能であるということは、公衆による利用可能性が非常に高いことを意味しており、この事実により当該特定の電子情報の証拠力は飛躍的に高まることとなる。

なお、上で述べたネットワークにはインターネットが最も適用し易く、その場合、電子情報はＨＴＭＬ（Hyper Text Markup Language）、ＸＭＬ（eXtensible Markup Language）等のマークアップ・ランゲージにより記述された文書であり

、ネットワーク上における電子情報の所在に関する情報はユニフォーム・リソース・ロケータ（ＵＲＬ）であり、アクセス条件は、少なくともアクセス元のＩＰアドレスを含むとすることが可能である。

【０００６】

本発明の第３の態様に係る、ネットワークに接続された特定のコンピュータにおいて特定の電子情報が公開されていたことを証明するシステムは、記録依頼に応じて、特定のコンピュータに格納された当該特定の電子情報へアクセスし、特定の電子情報をコピーする手段と、コピーされた特定の電子情報及びネットワーク上における特定の電子情報の所在に関する情報を含む属性情報を日時と共にユニークに特定し且つ認証する電子証明書を取得し、当該電子証明書及び属性電子情報を記憶装置に格納する手段と、記憶装置に格納された電子証明書及び属性電子情報を提供する手段とを有する。

また、本発明の第４の態様に係る電子情報公開証明システムは、記録依頼に応じて、特定のコンピュータに格納された特定の電子情報へ所定のタイミングでアクセスし、アクセスするごとに特定の電子情報をコピーするアクセス手段と、コピーされた特定の電子情報及びネットワーク上における特定の電子情報の所在に関する情報とアクセス条件とを含む属性情報を日時と共にユニークに特定し且つ認証する電子証明書を取得し、当該電子証明書及び属性情報を記憶装置に格納する手段と、記憶装置に格納された電子証明書及び属性情報を当該証明依頼元に提供する発行手段とを有する。

本発明の第４の態様において、電子証明書を発行する手段をさらに有するような構成も可能である。

なお、本発明の第２の態様について説明した第２の態様の変形例を、第４の態様に係る電子情報公開証明システムに対して応用することも可能である。

さらに、本発明の第１及び第２の態様に係る電子情報公開証明方法をコンピュータで実行するためのプログラムとして実装することが可能であり、このプログラムは、例えばフロッピー・ディスク、ＣＤ－ＲＯＭ、光磁気ディスク、半導体メモリ、ハードディスク等の記憶媒体又は記憶装置に格納される。

【０００７】

【発明の実施の形態】

まず、本発明の前提に係わる提供されるサービスの概略を説明しておく。例えば、依頼人Ａは、（１）インターネットに接続された自己のＷＷＷ（World Wide Web）サーバに格納されたホームページが、インターネット上で相当期間公開されていることを記録すること、及び（２）ホームページの存在及びその存在場所を公衆が知り得るようにするため当該ホームページにリンクを貼ることを、本サービスの提供者Ｂに依頼する、ものとする。

本依頼を受けたサービス提供者Ｂは、依頼人Ａの知らない任意のタイミングで、指定されたＵＲＬのホームページに、依頼人Ａの知らないＩＰアドレスからアクセスし、当該ホームページをコピーする。次に、サービス提供者Ｂは、ホームページのＵＲＬ及びアクセス元のＩＰ（Internet Protocol）アドレス等を含む属性情報を生成し、ホームページのコピー及びその属性情報を、日時と共にユニークに特定し且つ認証する電子証明書を取得する。そして、サービス提供者Ｂは、ホームページのコピー及び属性情報と、取得した電子証明書とを対応付けて保存する。

サービス提供者Ｂは、依頼人Ａの知らない任意のタイミングで、再度指定されたＵＲＬのホームページにアクセスし、当該ホームページをコピーする。この際、アクセス元のＩＰアドレスを変更してアクセスすることにより、依頼人ＡのＷＷＷサーバがアクセス制限をしていないという証明を付加的に得ることができる。次に、サービス提供者Ｂは、上と同じように属性情報を生成し、ホームページのコピー及びその属性情報を日時と共にユニークに特定し且つ認証する電子証明書を取得する。そして、サービス提供者Ｂは、ホームページのコピー及び属性情報と、取得した電子証明書とを対応付けて保存する。サービス提供者Ｂは、このような処理を依頼人Ａの指定した相当期間繰り返す。

また、サービス提供者Ｂは、（２）の依頼に対し、指定されたホームページのＵＲＬへのリンクをインターネットに接続された自己のＷＷＷサーバのホームページに掲載し、一般公衆がアクセス可能にする。例えば、当該リンクを、依頼人ごと、又は内容の分野毎に検索できるようにしておく場合もある。なお、ＷＷＷサーバにリンクを掲載していたことについても掲載期間等と共に記録を残してお

く。

依頼人Ａは、上の依頼と同時に又は必要となった時に、上の（１）で指定したホームページに対する記録内容の提供をサービス提供者Ｂに申し込むことができる。この申込みに対応してサービス提供者Ｂは、保存したホームページのコピー及び属性情報と電子証明書とを依頼人Ａに提供する。この際、例えばＣＤ－Ｒ等に上で述べたデータを書き込んで提供することも可能であるし、インターネットを介して提供することも可能である。さらに、上の（２）の結果として、サービス提供者ＢのＷＷＷサーバに、指定したホームページへのリンクが掲載されていたこと及びその期間等についての記録を証明書として、依頼人Ａに提供する場合もある。

依頼人Ａは、サービス提供者Ｂから提供を受けた情報を当該ホームページがインターネット上で相当期間公開していたことの証明として使用することができる。

【０００８】

依頼人Ａは、上で述べた（１）及び（２）の他に、（３）インターネット上の一般公衆向け検索エンジンで、指定したホームページが検索できるということの記録をサービス提供者Ｂに依頼することもできる。これは、ホームページの存在及び存在場所を公衆がより知り易い状態にあったことの証拠となる。サービス提供者Ｂは、任意の検索エンジンで、適切なキーワード等で検索を行う。指定されたホームページが検索できた場合には、当該検索できたという事実及び使用した検索エンジンのアドレス及び名称、並びに使用したキーワード、検索日時等を記録する。この記録を証明書として、記録内容提供依頼に応じて、依頼人Ａに提供する場合もある。

依頼人Ａは、（１）では自己のＷＷＷサーバに格納されたホームページについて記録することを依頼していたが、（１）’他人のＷＷＷサーバに格納されたホームページについて記録することをサービス提供者Ｂに依頼できる。この場合、サービス提供者Ｂは上の（１）で述べたような処理を同じように実施する。しかし、他人のＷＷＷサーバのホームページが、依頼人Ａの指定した相当期間中存在し続ける保証は無く、存在しなくなってしまったり、改変される場合もある。存

在しなってしまった場合には、サービス提供者Ｂは、インターネット上で公開が確認された期間を記録し、依頼人Ａの記録内容提供依頼に応じて、通常提供する情報に加え当該期間を提供する場合もある。改変される場合には、上で述べた処理を実施すれば、改変の履歴が残る。なお、他人のＷＷＷサーバに格納されたホームページは、依頼人ＡがそのＵＲＬを指定してもよいし、例えば指定された検索エンジンで指定されたキーワード検索を行った結果の全てのＵＲＬといった指定も可能である。

また、依頼人Ａは、（４）自己又は他人のＷＷＷサーバに格納されたホームページのバージョン遷移の記録をサービス提供者Ｂに依頼することもできる。サービス提供者Ｂは、（１）と同じ処理を実施する。但し、サービス提供者Ｂは、前回アクセスした時のホームページの内容と、今回アクセスした時のホームページの内容とが異なるかを検査する。異なる場合には、例えば、以前と異なっていたということを記録する。

なお、サービス提供者Ｂがホームページのコピーを保存する必要は無い。例えば依頼人Ａが保存すれば良い。サービス提供者Ｂがホームページのコピーを保存しない場合には、（１）及び（１）’の処理でアクセス毎に保存されるのは、属性情報と電子証明書だけである。また、（４）の場合、前回アクセスした時のホームページの内容と今回アクセスした時のホームページの内容が異なっていた場合、その差分を保存する又は異なっていた場合にのみホームページ全体を保存する等により、バージョンの変更を保存することができる。

また（１）及び（１）’の記録依頼における記録期間、回数、頻度等は、依頼人Ａにより指定できる。サービス提供者Ｂはそれに従って記録を行う。

さらに、（２）乃至（４）のサービスはオプションとすることができ、特に（２）及び（３）といったサービスは、他の媒体等でホームページの存在及び所在が公衆に明らかになっていれば必要ない。

【０００９】

一方サービス提供者Ｂは、本サービスを続けていくと、インターネットを介して公開されていたという電子証明書付きのホームページを多数保持することになる。この情報を用いて、サービス提供者Ｂは、（５）電子証明書付きのホームペ

ージ提供サービスを行うことができる。例えば、サービス提供者Ｂは、インターネットを介してキーワード検索等ができるようなデータベースを構築し、第３者に検索サービスを提供する。そして検索者Ｓの記録内容提供依頼に応じて、インターネットを介して又はＣＤ－Ｒのような媒体で、記録内容を提供する。また、電子証明書付きのホームページの要約を作成し、その要約で検索のスクリーニングができるような形態にデータベースを構築する場合もある。

以上のようなサービスを提供するための電子情報公開証明システムの概要を図１に示す。ネットワーク１には、３で示すサーバＡ、５で示すサーバＢ、７で示すサーバＣ、９で示すサーバＤ、１１で示すサーバＥ及び図示されない多数のコンピュータが接続されている。ネットワークである１は例えばインターネットである。３で示すサーバＡは、WWWサーバであり、電子情報、例えばＵＲＬがhttp://www.abcd.co.jpであるホームページ３１を格納しており、ネットワーク１で公開している。

５で示すサーバＢは、サービス提供者が管理するサーバであり、依頼人指定の電子情報にアクセスし、コピーを取得するコピー取得機能５１と、例えばＵＲＬ等の電子情報の所在に関する情報及びアクセス条件を含む属性情報を生成する属性情報生成機能５３と、電子情報のコピー及び属性情報を日時と共にユニークに特定し且つ認証する電子証明書を取得する証明書取得機能５５と、必要な情報を保存する保存機能５７と、依頼人の申し出に対応して保存されている電子証明書等を提供するための証明書提供機能５９とを含む。この５で示すサーバＢには記憶装置６１が接続されている。

７で示すサーバＣは、特定の電子情報を日時と共にユニークに特定し且つ認証する証明書を発行するタイムスタンプ証明書発行機能７１を有している。７で示すサーバＣは、ネットワーク１を介して証明書発行依頼を受け取り、タイムスタンプ証明書発行機能７１にて電子証明書を発行し、依頼元に電子証明書を送り返す。

【００１０】

９で示すサーバＤは、５で示すサーバＢに機能を付加するためのサーバであって、例えばWWWサーバとして依頼人が指定したホームページへのリンク９１を

掲載する。但し、このようなリンク９１のデータベースを作成し、リンク先ホームページの内容又は所有者等毎に検索可能にしておく場合もある。さらに、５で示すサーバＢに接続されている記憶装置６１のデータを用いてデータベース９５を作成し、９で示すサーバＤがこのデータベース９５をネットワークを介して検索可能にする検索機能９３を保持している場合もある。さらに、記憶装置６１のデータから各電子情報の要約を作成し、この要約に関するデータベース９７を検索機能９３がネットワークを介して検索可能にする場合もある。

１１で示すサーバＥは、一般公衆向け検索エンジンである。この一般公衆向け検索エンジンは、従来と変わらないので説明は割愛する。

次に、本発明により提供されるサービスの概要（１）及び（１）'を、図１に示したシステムの動作として説明する。

依頼者Ａは例えば３で示すサーバＡのＵＲＬ　http://www.abcd.co.jpのホームページを相当期間記録すべき電子情報として指定し、サービス（１）又は（１）'をサービス提供者Ｂに依頼する。サービス提供者Ｂは５で示すサーバＢを用いて処理を行う。５で示すサーバＢのコピー取得機能５１は、任意のタイミングで図１のサーバＡに示したhttp://www.abcd.co.jpに例えばルート（Ａ）によりアクセスし、ホームページ３１のコピーを例えばルート（Ｂ）を介して取得する。コピーは、例えば５で示すサーバＢのメインメモリに保持される。コピー取得機能５１は、アクセス毎に、アクセス元のＩＰアドレスを記憶装置に記憶しておく。コピー取得機能５１は、アクセス条件を決定する機能を含んでおり、例えば依頼人が指定した相当期間中、どのタイミングで且つどのアクセス元ＩＰアドレスを使用してアクセスするか決定する。また、依頼人が頻度を指定している場合には、当該頻度の指定を満たすように、アクセスをスケジューリングする。

属性情報生成機能５３は、このアクセス元のＩＰアドレスと依頼人Ａ指定のＵＲＬとを含む属性情報を生成する。属性情報には、ＩＰアドレス及びＵＲＬのほかに、例えば５で示すサーバＢが図示しないプロキシ・サーバを介してネットワーク１に接続している場合には、このプロキシ・サーバのＩＰアドレスや、アクセス日時を含むようにしてもよい。

【００１１】

証明書取得機能５５は、取得したホームページ３１のコピー及び生成した属性情報に対して電子証明書を取得する。より具体的な処理については後に詳述する。図１のシステムでは、証明書取得機能５５は、ネットワーク１の例えばルート（Ｃ）を介して発せられる電子証明書発行依頼を、７で示すサーバＣのタイムスタンプ証明書発行機能７１にて受領し、タイムスタンプ証明書機能７１により発行される電子証明書をネットワーク１の例えばルート（Ｄ）を介して受領する。タイムスタンプ証明書発行機能７１については後に詳しく述べるものとする。

保存機能５７は、コピー取得機能５１が取得したホームページ３１のコピーと、属性情報生成機能５３が生成した属性情報と、証明書取得機能５５が取得した電子証明書とを、記憶装置６１に格納する。但し、コピー取得機能５１が取得したホームページ３１のコピーを保存することは任意である。例えば、依頼人Ａが自分で保存する場合もあるからである。また、保存機能５７は、前回コピーしたホームページ３１の内容と、今回アクセスしたホームページ３１の内容が同一である場合、今回取得したホームページ３１のコピーを保存しないといった判断を行うようにしてもよい。また、保存機能５７は、後に証明書提供機能５９が必要なデータを取り出し易いように、依頼人毎又は指定されたＵＲＬ毎にデータを保存しておく。

記録依頼と同時又は任意のタイミングで依頼人Ａは記録内容の提供を申し出る。この際、証明書提供機能５９は、それに応じて、依頼の対象となるホームページ３１のコピー、属性情報及び電子証明書を記憶装置６１から読み出し、図１の例ではＣＤ－Ｒ６３等の記憶媒体に格納して、依頼人Ａに提供する。なお、ホームページ３１のコピー、属性情報及び電子証明書は、アクセス毎に記憶されるが、証明書提供機能５９はこれらを全てＣＤ－Ｒ等の記憶媒体に格納して提供してもよいし、ホームページ３１のコピーに変化がない場合には、最初のアクセス時のホームページ３１のコピーと全ての属性情報及び全ての電子証明書を提供するようにしてもよい。さらに、証明書提供機能５９において、属性情報及び電子証明書を用いて、ＵＲＬ、アクセス元ＩＰアドレス及び証明書日時を含むアクセス記録を作成し、当該アクセス記録と、最初のアクセス時のホームページ３１と、全ての属性情報と、全ての電子証明書とをサービス提供者Ｂによる証明書として

提供するようにすることも可能である。なお、保存機能５７がホームページ３１のコピーを保存しない場合には、当然証明書提供機能５９も依頼人Ａにホームページ３１のコピーを提供しない。

【００１２】

次に、本発明により提供されるサービスの概要（２）を、図１に示したシステムに基づき説明する。（２）は、ホームページの存在及びその存在場所を公衆が知り得るようにするため当該ホームページにリンクを貼ることを、依頼人Ａがサービス提供者Ｂに依頼するものである。

この依頼に応じてサービス提供者Ｂは、ネットワーク１に接続された９で示すサーバＤに、３で示すサーバＡに格納されたホームページ３１へのリンク９１を掲載する。依頼数が少なければ、９で示すサーバＤに格納されたホームページに、単に指定されたホームページのＵＲＬを掲載するだけでも良い。しかし、依頼数が多い場合には、リンクについてのデータベースを構築し、ネットワーク１を介して、第三者が、ホームページの内容又は依頼人の業種等によって検索できるようにする場合もある。サービス提供者Ｂは、ホームページ３１へのリンク９１を自己のホームページに掲載していた期間や、検索可能であった期間を記憶装置に記録しておき、後に依頼人Ａ等から求められた時には、当該記録を証明書として提供する。

次に、本発明により提供されるサービスの概要（３）を、図１に示したシステムに基づき説明する。（３）は、ネットワーク１上の一般公衆向け検索エンジンである１１で示すサーバＥで、指定したホームページが検索できるということの記録をサービス提供者Ｂに依頼をするものである。

サービス提供者Ｂは、例えば５で示すサーバＢを介して、１１で示すサーバＥにおける検索エンジンで、適切なキーワード等により検索を行い、指定されたホームページ３１が検索できた場合には、当該検索できたという事実及び１１で示すサーバＥの名称及びアドレス、使用したキーワード、検索日時等を記録する。後に依頼人Ａ等から求められた時には、この記録を証明書として提供する。

次に、本発明により提供されるサービスの概要（４）を、図１に示したシステムに基づき説明する。（４）は、ホームページ３１のバージョン遷移の記録をサ

ービス提供者Ｂに依頼するものである。

サービス提供者Ｂは、５で示すサーバＢを用いて（１）と同様な処理を行う。すなわち、所定のタイミングで３で示すサーバＡのホームページ３１にアクセスし、ホームページ３１のコピーを取得する。次に、ＵＲＬ及びアクセス条件を含む属性情報を生成し、属性情報及びホームページ３１のコピーに対し電子証明書を取得する。そして、少なくとも属性情報及び電子証明書を記憶装置６１に保存する。ホームページ３１のコピーを記憶装置に保存するようにすることも可能である。次に、所定のタイミングにて３で示すサーバＡのホームページ３１にアクセスし、同様な処理を行い、属性情報及びホームページ３１のコピーに対し電子証明書を取得する。そして、前回アクセスした時のホームページ３１、より正確には、最も最近変更が検出された時のホームページ３１、の内容と、今回アクセスした時のホームページ３１の内容が異なっているか判断する。この判断は、コピー取得機能５１が行っても、保存機能５７が行ってもかまわない。内容が異なっている場合には、少なくとも属性情報及び電子証明書に加え、異なっていたということを記憶装置に記録する。場合によっては、前回アクセスした時のホームページ３１の内容と今回アクセスした時のホームページ３１の内容の差分を記憶装置に記録するようにしてもよいし、異なっている場合には、必ずホームページ３１の全体のコピーを記憶装置に保存するようにしてもよい。

依頼人Ａ等から求められたときには、サービス提供者Ｂは、証明書提供機能５９により、少なくとも属性情報及び電子証明書と変更の有無の記録を提供する。差分や異なる毎にホームページ全体を提供してもよい。

【００１３】

次に、本発明により提供されるサービスの概要（５）を、図１に示したシステムに基づき説明する。（５）は、電子証明書付のホームページ提供サービスである。

サービス提供者Ｂは、９で示すサーバＤに検索機能９３を設け、記憶装置６１に蓄えられた電子証明書及び属性情報付きのホームページ３１のコピーを使用して、データベース９５を作成する。そして、第三者に検索機能９３からデータベース９５を検索できるようにする。第三者が使用を欲するホームページ３１のコ

ピーを見つけた場合には、ネットワーク１等を介して、記録内容提供依頼をサービス提供者Ｂに提出する。サービス提供者Ｂは、証明書提供機能５９を使用して、例えばＣＤ－Ｒ６３等に提供を求められたホームページ３１のコピー及び属性情報並びに電子証明書を格納し、当該ＣＤ－Ｒ６３等を提供する。ネットワーク１を介して上述のようなデータを送信するようにしてもよい。

さらに、サービス提供者Ｂは、ホームページ３１のコピーからその要約を作成し、要約のデータベース９７を構築し、検索機能９３により第三者が検索可能にすることも可能である。第三者は、要約のデータベースでスクリーニングをしたのちに、ホームページ３１のコピーを確認し、必要な電子情報の記録内容提供依頼を出すことができるようになる。

本発明の主要なサービス（１）及び（１）'の処理フローを図２にまとめた。依頼人Ａから、例えばホームページ等の記録対象電子情報に関する、例えばＵＲＬ等の所在に関する情報及び例えば記録期間等の記録条件を指定した記録依頼がサービス提供者Ｂに提出された場合（ステップＳ１）には、記録条件に合致するようにコピー取得機能５１は、アクセス条件を決定（ステップＳ３）し、当該ＵＲＬに所定のタイミングで所定のアクセス元ＩＰアドレスからアクセスして、ホームページのコピーを取得（ステップＳ５）する。そして、属性情報生成機能５３は、ホームページのＵＲＬとアクセスの条件としてアクセス元ＩＰアドレスとを含む属性情報を生成（ステップＳ７）する。

その後、証明書取得機能５５は、属性情報及び取得したホームページのコピーを日時と共に特定し且つ認証する電子証明書を、タイムスタンプ証明書発行機能７１から取得（ステップＳ９）する。なお、５で示すサーバＢが、タイムスタンプ証明書発行機能７１を含むような構成とすることも可能であって、その場合証明書取得機能５５はタイムスタンプ証明書発行機能７１に置き換えられる。

そして、保存機能５７は、少なくとも属性情報及び電子証明書を記憶装置６１に格納（ステップＳ１１）する。なお、上でも述べたが、ホームページのコピーを記憶装置に保存するかは任意である。そして、この処理を記録終了の条件が満たされるまで繰り返す（ステップＳ１３）。記録終了の条件とは、例えば依頼人Ａの指定した記録期間が終了した場合や、依頼人Ａの指定した記録回数に達した

場合等である。

【００１４】

図３に本発明の主要なサービス（１）及び（１）'に加え（４）のサービスを合わせて行う場合の処理フローの一例を示す。

依頼人Ａから、例えばホームページ等の記録対象電子情報の、例えばＵＲＬ等の所在に関する情報及び例えば記録期間等の記録条件を指定した記録依頼がサービス提供者Ｂに提出された場合（ステップＳ２１）に、記録条件に合致するようにコピー取得機能５１は、アクセス条件を決定（ステップＳ２３）し、当該ＵＲＬに所定のタイミングで所定のアクセス元ＩＰアドレスからアクセスして、ホームページのコピーを取得（ステップＳ２５）する。そして、属性情報生成機能５３は、ホームページのＵＲＬとアクセスの条件としてアクセス元ＩＰアドレスとを含む属性情報を生成（ステップＳ２７）する。

その後、証明書取得機能５５は、属性情報及び取得したホームページのコピーを日時と共に特定し且つ認証する電子証明書を、タイムスタンプ証明書発行機能７１から取得（ステップＳ２９）する。なお、５で示すサーバＢが、タイムスタンプ証明書発行機能７１を含むような構成とすることも可能である。

ここでは次に保存機能５７が、前回アクセスした時のホームページの内容と、今回アクセスした時のホームページの内容に変更が無いか検査（ステップＳ３１）する。この検査は、記憶装置６１に格納された最も最近変更が検出された時のホームページのコピーを読み出し、今回アクセス時のホームページのコピーとを比較することにより行われる。変更を検出した場合には、ホームページのコピーと電子証明書と属性情報とを関連付けて記憶装置に保存（ステップＳ３３）する。一方、変更が検出されない場合には、証明書及び属性情報を記憶装置に保存（ステップＳ３５）する。このような処理が記録終了の条件が満たされるまで繰り返される（ステップＳ３７）。

図３のような処理フローが行われたときには、例えば図４のような情報が保存されることになり、指定されたＵＲＬのホームページの遷移を証明することができる。図４で、初回のアクセス時には、全て変更ということで、ホームページのコピーと電子証明書と属性情報とを記憶装置に保存する。二回目のアクセス時に

は、初回のアクセス時に保存したホームページのコピーと今回アクセスした時に取得したホームページのコピーを比較し、変更が無いと判断され、電子証明書及び属性情報のみが保存される。三回目のアクセス時には、初回のアクセス時に保存したホームページのコピーと今回アクセスした時に取得したホームページのコピーを比較し、変更が無いと判断され、電子証明書及び属性情報のみが保存される。四回目のアクセス時には、初回のアクセス時に保存したホームページのコピーと今回アクセスした時に取得したホームページのコピーを比較し、変更があると判断され、四回目のアクセス時に取得したホームページのコピーと、電子証明書と、属性情報とが保存される。以下同様な処理が変更あり又は無しの場合に行われる。比較の対象は、最も最近の変更を検出したため保存を実行したホームページのコピーとなる。

【００１５】

次に依頼人Ａによる記録内容提供依頼に応じて実行される処理フローの例を図５に示す。記録内容提供依頼（ステップＳ４１）には対象となる電子情報が含まれているので、まず証明書提供機能５９は、対象となる電子情報を特定（ステップＳ４３）する。そして、証明書提供機能５９は、記憶装置６１から対象電子情報のコピーと、電子証明書及び属性情報を読み出す（ステップＳ４５）。なお、記録依頼が１回だけの記録を要求していたり、結果的に１回アクセスしただけで対象電子情報が無くなったりする場合には、読み出されるデータは１セットのみであるが、通常複数回に渡って記録しているので、電子情報のコピーと属性情報と電子証明書のセットを複数読み出すことになる。

そして、証明書提供機能５９は、公開期間の計算を付加的に行う（ステップＳ４７）。電子証明書には日時の記録が含まれるので、初回アクセス時に取得した電子証明書と最後にアクセスした時に取得した電子証明書とを参照すれば、少なくともいつからいつまで公開されていたか分かるので、この情報を公開期間とする。但し、この処理は任意である。

最後に、証明書提供機能５９は、対象電子情報のコピーと、電子証明書及び属性情報、並びに公開期間情報を、例えばＣＤ－Ｒ等の媒体に格納して提供（ステップＳ４９）する。

【００１６】

ここで電子証明書について図６を用いて簡単に説明しておく。本発明では、電子情報を日時と共にユニークに特定し且つ認証する電子証明書を発行するものであれば、どのような方式にて電子証明書を発行してもよい。よって、以下の説明は一例であって、他の方式にて電子証明書を発行することにしてもかまわない。

電子情報１０１を電子証明書の対象であるとすると、まず、電子情報１０１に対してハッシュ値１０３を計算する。ハッシュ関数は一方向関数であれば何でも良い。ハッシュ値の計算までを例えば証明書取得機能５５が行う。そして、このハッシュ値１０３を含む証明書発行依頼を、タイムスタンプ証明書発行機能７１に送る。タイムスタンプ証明書発行機能７１は、同じように送られてきた他のハッシュ値と共に処理をする。例えば図６のように、２つのハッシュ値からもう一つのハッシュ値を生成するといった処理を繰り返し、送られてきた全ハッシュ値から最終的に一つのハッシュ値１０６を生成する。このハッシュ値１０６と、時刻Ｔ－１（Ｔは整数）におけるＳＨＶ（Super Hash Value:スーパー・ハッシュ値）１０５とを用いて時刻ＴにおけるＳＨＶ１０７を生成する。このようにして生成された時刻ＴにおけるＳＨＶ１０７とハッシュ値１０３と、時刻Ｔの時刻情報と、文書ＩＤとが電子証明書１０９を構成する。この電子証明書１０９はハッシュ値１０３の送り主に送信され、電子情報１０１と電子証明書１０９とを対にして、電子情報１０１を日時と共にユニークに特定し且つ認証することができるようになる。

なお、電子情報であるホームページを図６の電子情報とする場合には、ＨＴＭＬ文書が電子情報に当たる。よって、図７に示したように、ＨＴＭＬ文書１１０と、ＵＲＬ及びアクセス元ＩＰアドレスなどを含む属性情報１１１とからハッシュ値を計算し、このハッシュ値から電子証明書を作成することになる。但し、ホームページの内容が文章だけであればこれで十分であるが、通常ホームページには例えばＧＩＦファイル等の画像ファイル１１２が埋め込まれている。このような場合には、ＧＩＦファイル等の画像ファイルの内容もネットワーク上で公開されていた情報に含まれるため、この画像ファイルと、ＨＴＭＬ文書と、属性情報とからハッシュ値を計算するようにする。

さらに、ＨＴＭＬ文書に埋め込まれているのは、静止画像のみならず、動画像であったり、サウンドであったり、ブラウザのプラグイン等を必要とするフォーマットのファイルであったり、Ｊａｖａ（Sun Microsystems社の商標）アプレットであったりする。このようなオブジェクトが埋め込まれている場合には、これらのオブジェクトについても指定ＵＲＬアクセス時にコピーし、ハッシュ値計算に用いる。ハッシュ値を個々のファイルごとに計算しても、全てのファイルについて１つ計算してもよい。

【００１７】

このように本発明のサービスの概要（１）及び（１）'により、ネットワーク上で公開された電子情報に対し、公開されていたことを証明することができるようになる。（２）及び（３）により、一般公衆にその電子情報の存在及びその所在を知られるようになっていたことを証明することができるようになる。また、（４）により、電子情報のバージョン遷移を把握することができるようになる。さらに、（５）により、サービス提供者は電子証明書付き電子情報をより有効に使用することができ、依頼人は電子情報の公衆の利用を促進でき、第三者は自己が保持していなかった証拠力のある電子情報を取得することができるようになる。

このようなシステムにて、例えば特許の分野においては、属性情報及び電子証明書付き電子情報を、特許異議申立てや無効審判の証拠に使用することができるようになる。また、自己のホームページ等を公開技報のように用いることができるようになる。また、新規性の喪失の例外適用の証拠としても使用することができる。

以上述べた内容は一例であって様々な変形が可能である。例えば、５で示したサーバＢに含まれる５つの機能は、図１では１つのサーバに含まれるように示しているが、複数のサーバに分けて存在するようにすることも可能である。同様に、９で示したサーバＤでは、依頼されたホームページへのリンクを掲載し、且つ検索機能を設けているが、これらも別個のサーバにて実施されるようにすることも可能である。ネットワーク１に接続される一般公衆向け検索エンジンは１つに限定されない。また、ｈｔｔｐに限定されず、ｆｔｐでも対応することができる

。７で示したサーバＣの機能を５で示したサーバＢの機能に含めることも可能である。７で示したサーバＣによるサービスを行う主体と、５で示したサーバＢによるサービスを行う主体は、別でも同一でもよい。ネットワーク１はインターネットに限定されず、他の非排他的なアクセスを許可するネットワーク及びネットワーク利用を希望する者が非排他的に取り扱われるネットワークにまで拡大可能である。記録内容提供のための媒体をＣＤ－Ｒ６３としていたが、これも一例であって他の媒体、例えばＣＤ－ＲＯＭでも、ＤＶＤでもよい。

また図１に示した機能ブロックの分け方は一例であって、１つの機能ブロックを複数の機能ブロックに分けることも、複数の機能ブロックを１つの機能ブロックにまとめることも可能である。図１に示した機能ブロックの機能を実現するプログラムとコンピュータの組み合せにより図１のような装置を構成することも、一部又は全部を専用の電子回路等により実施することも可能である。

【００１８】

【発明の効果】

インターネット等のネットワーク上で、特定の電子情報が所定の条件の下公開されていたことを証明するための方法、システム及びコンピュータ・プログラム並びに該コンピュータ・プログラムを格納した記録媒体を提供することができた。

【図面の簡単な説明】

【図１】

本発明におけるシステムの概要を示すブロック図である。

【図２】

電子情報記録依頼に応じて行われる処理の一例を示すフローチャートである。

【図３】

電子情報記録依頼に応じて行われる処理の一例を示すフローチャートである。

【図４】

電子情報にアクセスするごとに保存する情報の種類の一例を示す模式図である。

【図５】

記録内容提供依頼に応じて行われる処理の一例を示すフローチャートである。

【図６】

電子情報を日時と共に特定し且つ認証する電子証明書の発行処理の一例を示す模式図である。

【図７】

図６の発行処理にて行われるハッシュ値の生成について説明するための模式図である。

【符号の説明】

１：ネットワーク

３：サーバＡ

５：サーバＢ

７：サーバＣ

９：サーバＤ

１１：サーバＥ

３１：ホームページ

５１：コピー取得機能

５３：属性情報生成機能

５５：証明書取得機能

５７：保存機能

５９：証明書提供機能

６１：記憶装置

６３：ＣＤ－Ｒ

７１：タイムスタンプ証明書発行機能

９１：リンク

９３：検索機能

９７：要約データベース

１０１：電子情報

１０３：ハッシュ値

１０５：時刻Ｔ－１におけるＳＨＶ

１０６：ハッシュ値

１０７：時刻ＴにおけるＳＨＶ

１０９：電子証明書

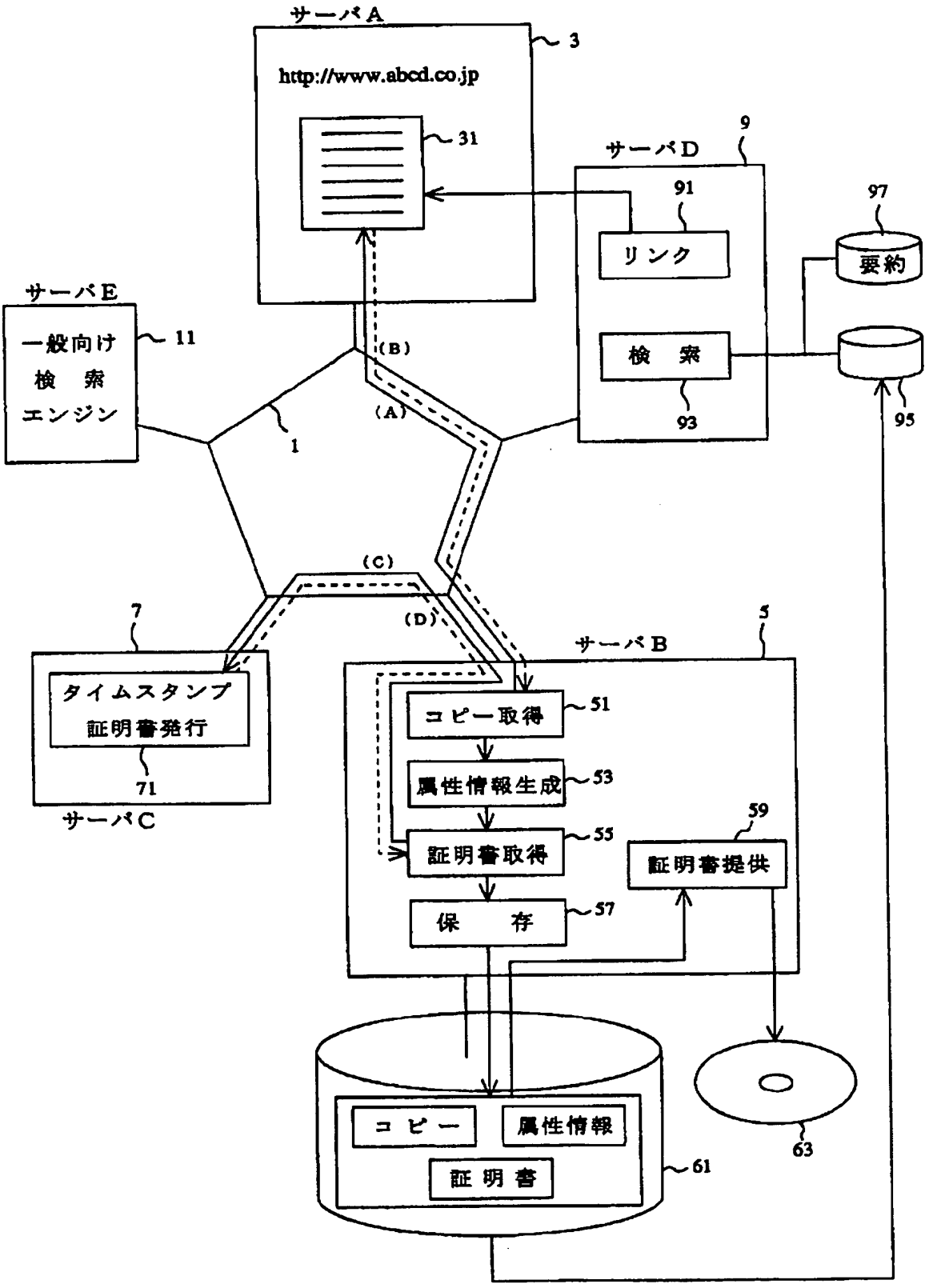
１１０：ＨＴＭＬ文書

１１１：属性情報

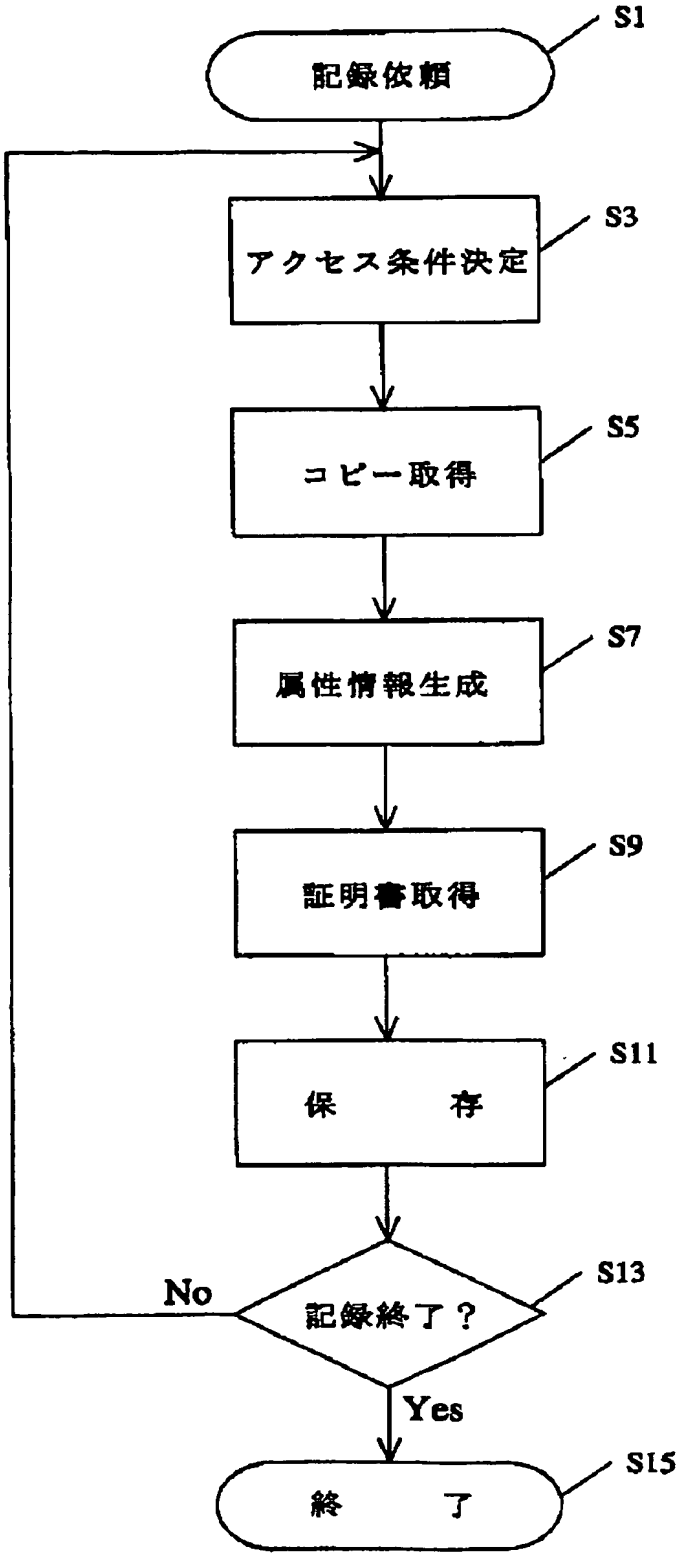
１１２：画像ファイル

【書類名】　図面

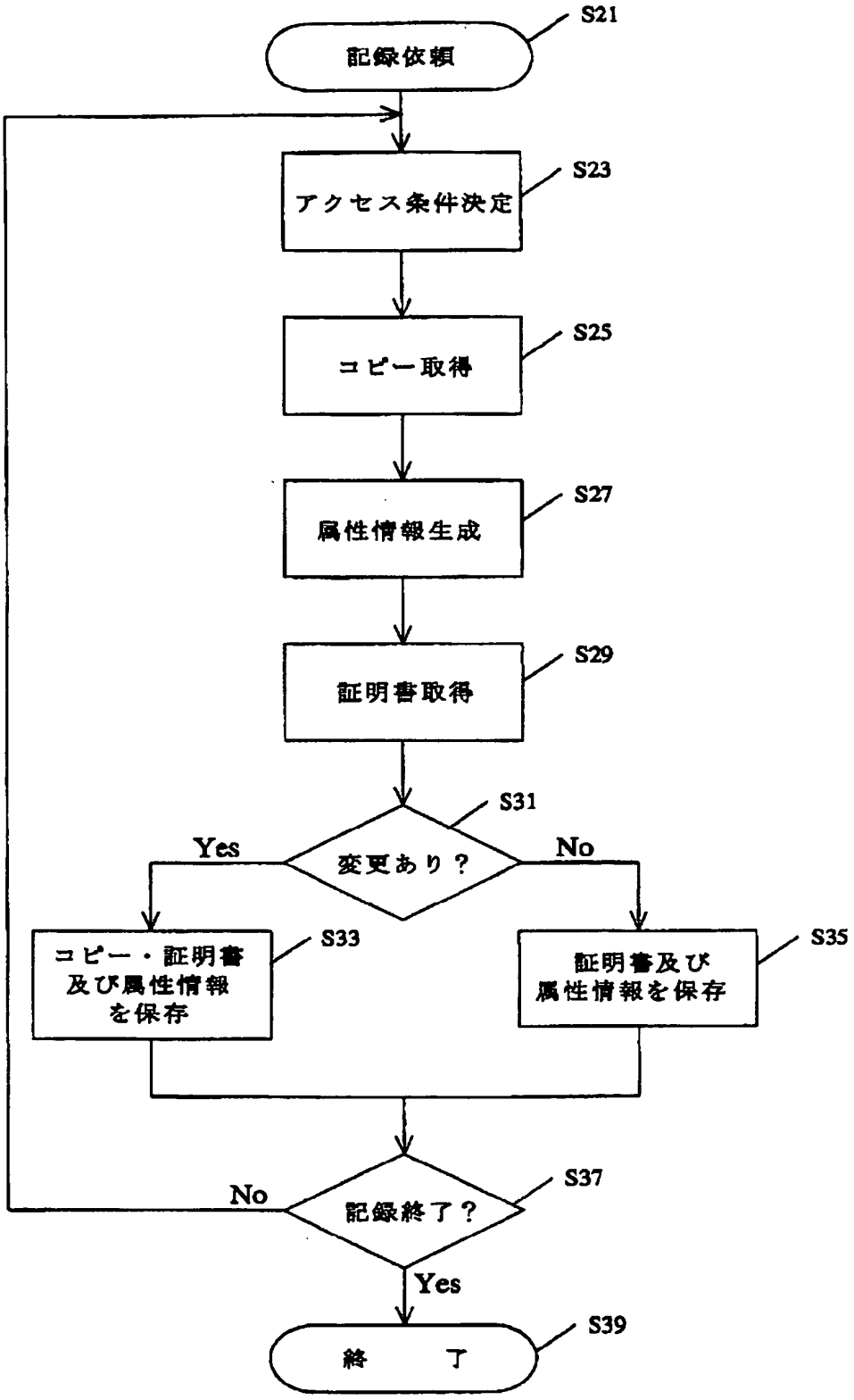
【図１】


サーバA
http://www.abcd.co.jp
3
31
サーバD
9
91
リンク
97
要約
サーバE
一般向け
検　索
エンジン
11
(B)
(A)
1
検　索
93
95
(C)
(D)
7
タイムスタンプ
証明書発行
71
サーバC
5
サーバB
コピー取得
51
属性情報生成
53
証明書取得
55
保　存
57
59
証明書提供
コピー
属性情報
証明書
61
63

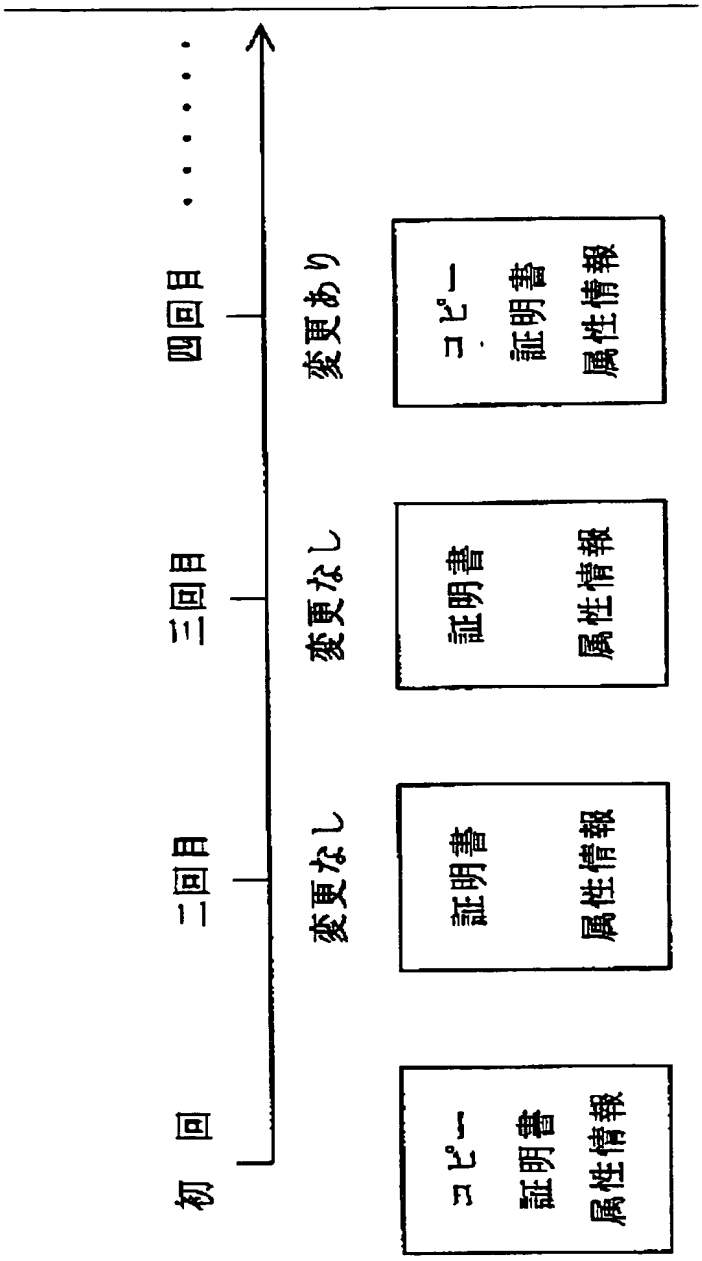
【図２】


S1
記録依頼
S3
アクセス条件決定
S5
コピー取得
S7
属性情報生成
S9
証明書取得
S11
保　　存
S13
No
記録終了？
Yes
S15
終　　了

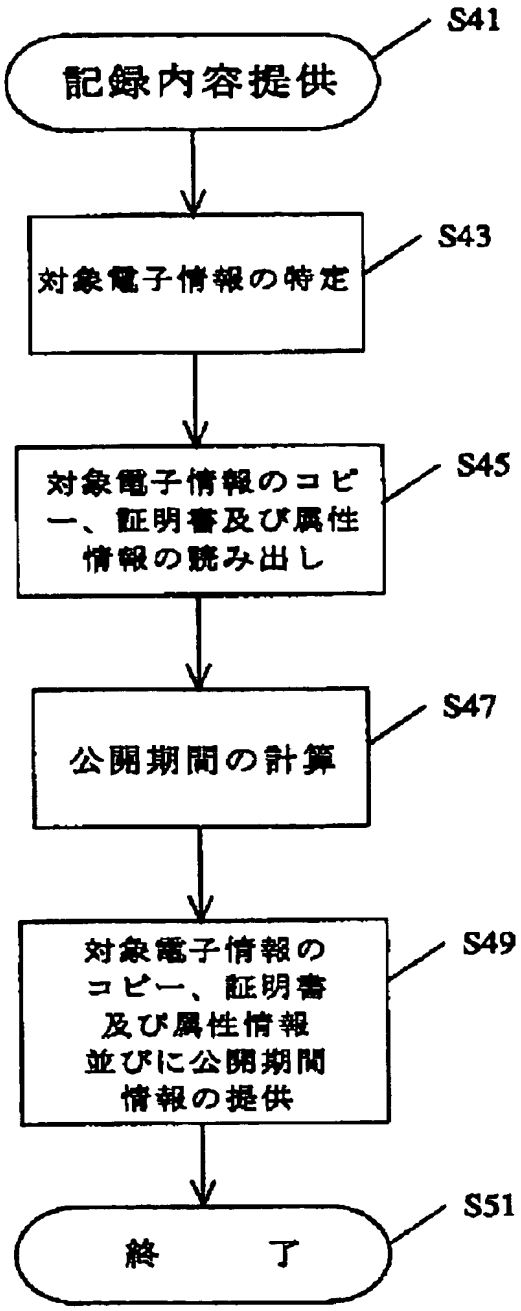
【図３】


S21
記録依頼
S23
アクセス条件決定
S25
コピー取得
S27
属性情報生成
S29
証明書取得
S31
変更あり？
Yes
No
S33
コピー・証明書及び属性情報を保存
S35
証明書及び属性情報を保存
S37
記録終了？
No
Yes
S39
終　了

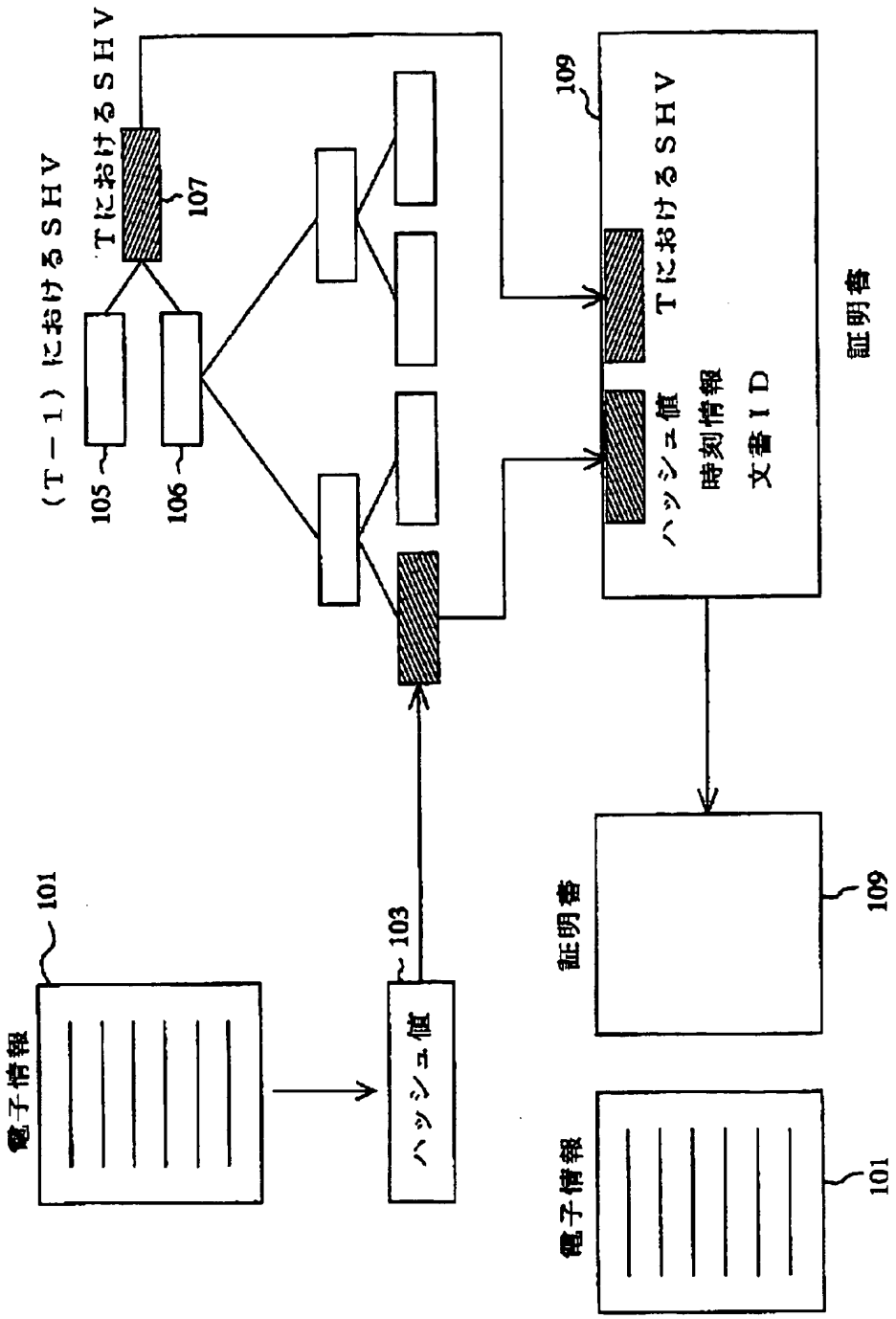
【図４】


初回
二回目
三回目
四回目
・・・・・・
変更なし
変更なし
変更あり
コピー
証明書
属性情報
証明書
属性情報
コピー
証明書
属性情報

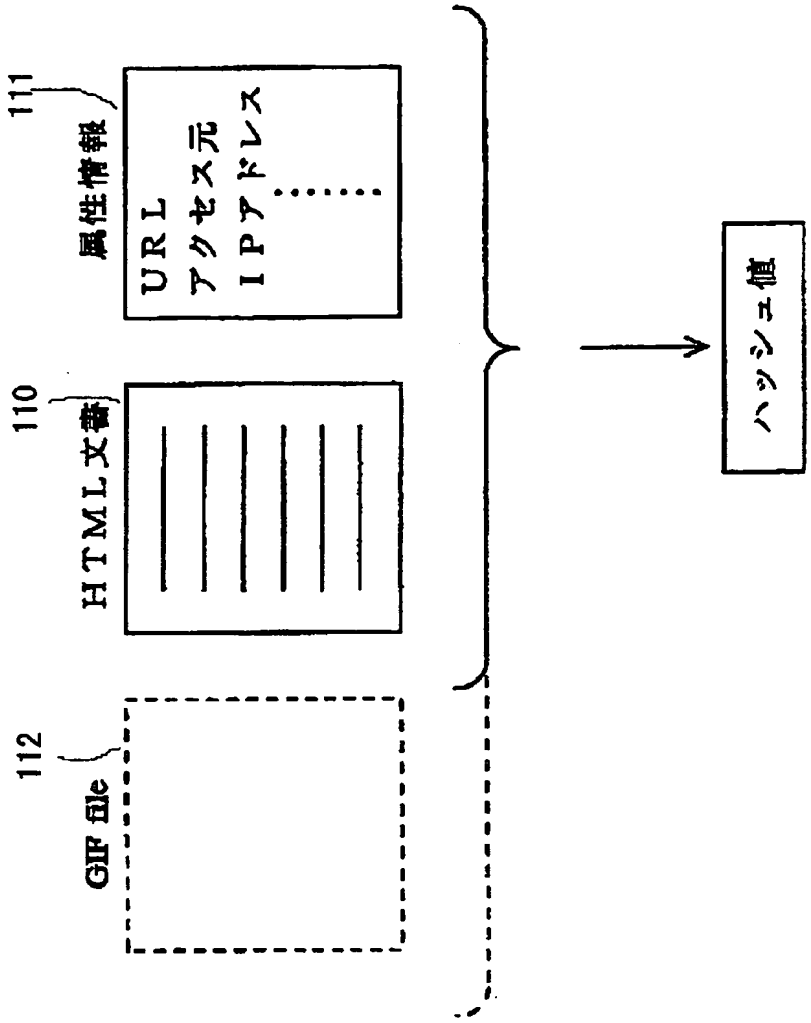
【図５】


S41
記録内容提供
S43
対象電子情報の特定
S45
対象電子情報のコピー、証明書及び属性情報の読み出し
S47
公開期間の計算
S49
対象電子情報のコピー、証明書及び属性情報並びに公開期間情報の提供
S51
終　了

【図６】


（Ｔ－１）におけるＳＨＶ
ＴにおけるＳＨＶ
107
105
106
109
ＴにおけるＳＨＶ
ハッシュ値
時刻情報
文書ＩＤ
証明書
101
電子情報
103
ハッシュ値
証明書
109
電子情報
101

【図７】



【書類名】　　要約書

【要約】

【課題】　インターネット等のネットワーク上で、ある電子情報が所定の条件の下公開されていたことを証明する。

【解決手段】　サービス提供者Ｂは、依頼人Ａから指定されたＵＲＬのホームページにアクセスし、当該ホームページをコピーし、ＵＲＬ及びアクセス元のＩＰアドレス等を含む属性情報を生成し、ホームページのコピー及びその属性情報を、日時と共にユニークに特定し且つ認証する電子証明書を取得し、ホームページのコピー及び属性情報と対応付けて保存する。これを指定された期間繰り返す。依頼人Ａは、依頼と同時に又は必要となった時に、指定したホームページに対する記録内容の提供をサービス提供者Ｂに申し込むことができる。この申込みに対応してサービス提供者Ｂは、保存したホームページのコピー及び属性情報と電子証明書とを依頼人Ａに提供する。また、サービス提供者ＢのWWWサーバに、指定したホームページへのリンクが掲載されていたこと及びその期間等についての記録を証明書として、依頼人Ａに提供する。

【選択図】　　図１

特願平１１－３４１２８８

出　願　人　履　歴　情　報

識別番号　［０００００６７４７］

１．変更年月日　１９９０年　８月２４日
［変更理由］　新規登録
住　所　東京都大田区中馬込１丁目３番６号
氏　名　株式会社リコー

２．変更年月日　２００２年　５月１７日
［変更理由］　住所変更
住　所　東京都大田区中馬込１丁目３番６号
氏　名　株式会社リコー